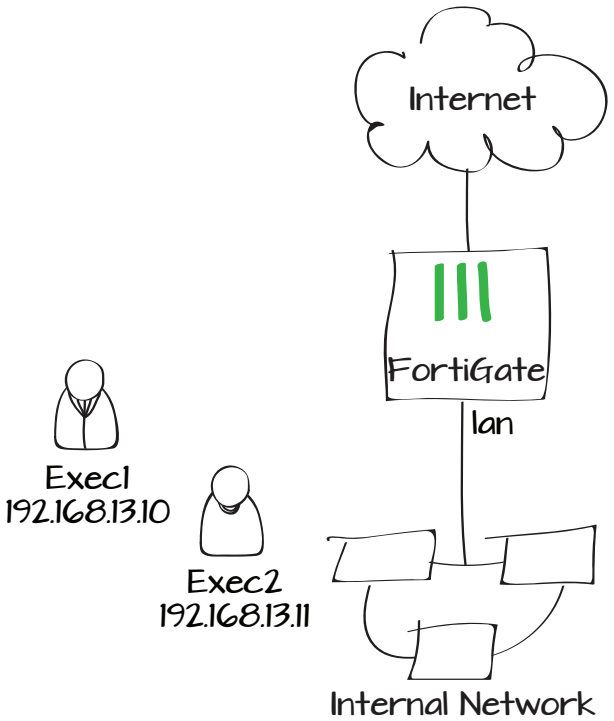
Excluding specific users from security scanning

In this example, two company executives will be excluded from the security scanning that is applied to all other Internet traffic. Since the executives connect to the Internet using the PCs that have static IP addresses, these addresses can be used to identify their traffic.

1. Applying security profiles to the staff policy
2. Creating firewall addresses and a group for the executives
3. Creating a security policy for the executives
4. Results

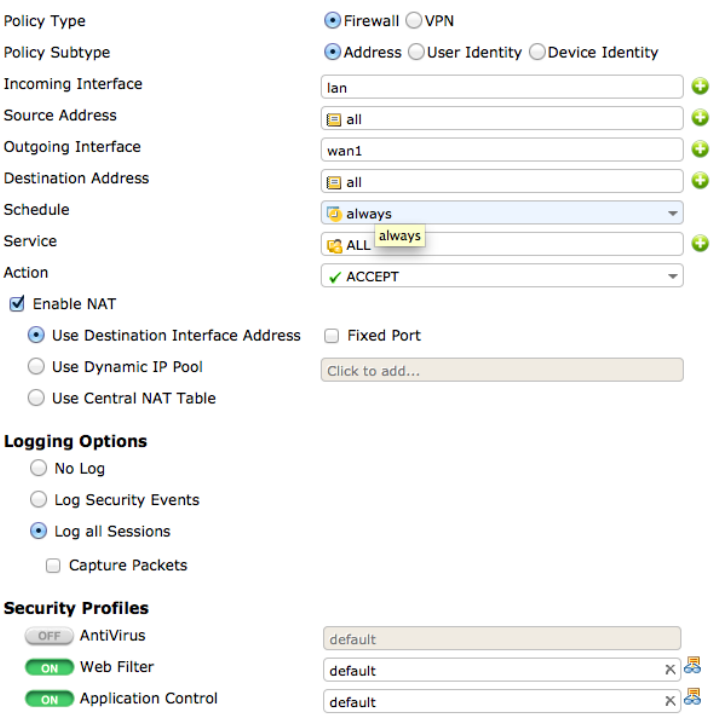


Applying security profiles to the staff policy

Go to **Policy > Policy > Policy** and edit the policy allowing Internet access. This policy will be used by the majority of the company's staff.

In order to view results, select **Log all Sessions**.

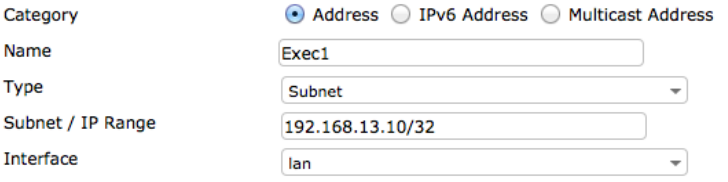
Under **Security Profiles**, enable **Web Filter** and **Application Control**. Set them to use the **default** profiles.



Creating firewall addresses and a group for the executives

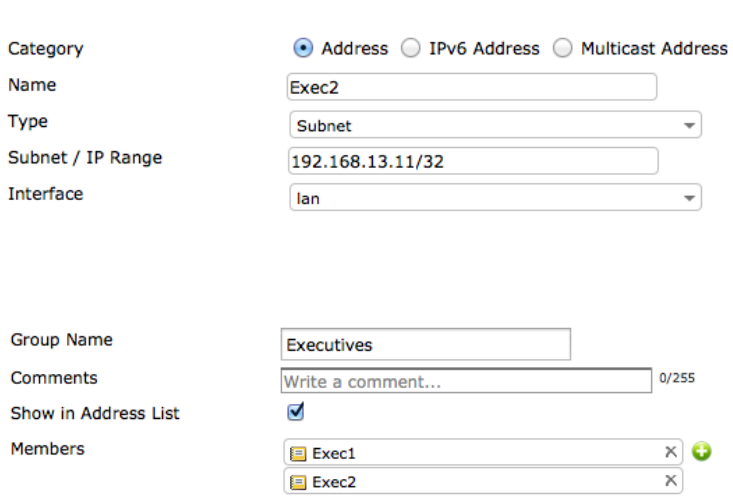
Go to **Firewall Objects > Address > Addresses**. Create an address for each executive.

Set **Type** to **Subnet** and **Interface** to **lan**. Set **Subnet/IP Range** to the static IP of the executive's PC. Use /32 as the Netmask to ensure that the firewall address applies only to the specified IP.



Go to **Firewall Objects > Address > Groups**.

Create a new group and add the new addresses as members.

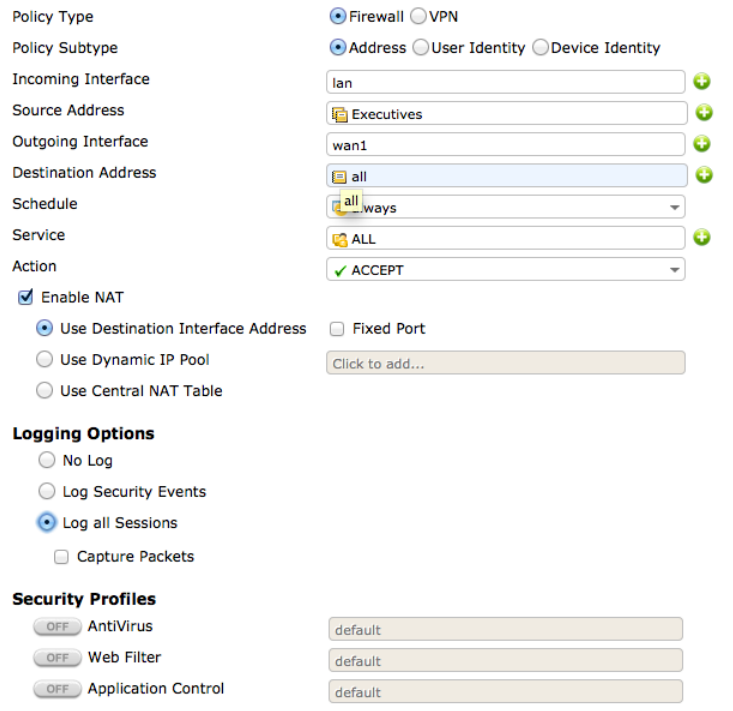


Creating a security policy for the executives

Go to **Policy > Policy > Policy**.

Create a policy allowing the executives to access the Internet. Set **Incoming Interface** to **lan**, **Source Address** to the firewall address group, and **Outgoing Interface** to your Internet-facing interface. **Enable NAT** and, in order to view results, select **Log all Sessions**.

Leave all **Security Profiles** disabled.



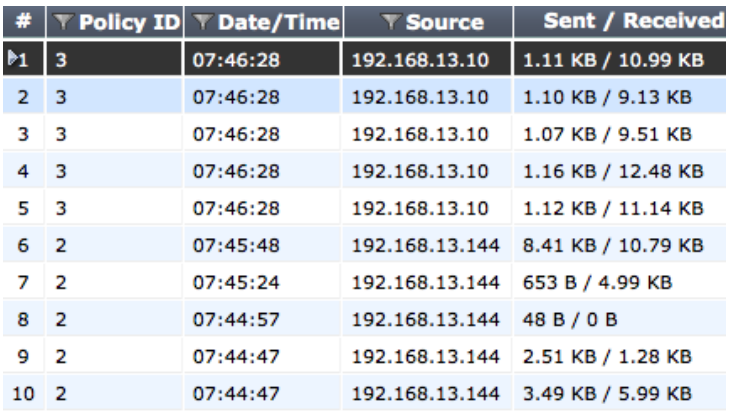
In the policy list, reorder the security policies by clicking and dragging the **Seq.#** column. Place the policy for the executives at the top of the list.

Seq.#	From	To	Source	Web Filter	Application Control	Action
1	lan	wan1	Executives			✓ Accept
2	lan	wan1	all	WEB default	APP default	✓ Accept
3	any	any	all			⊘ Deny

Results

Connect to the Internet from two computers on the internal network: one that has an IP address assigned to one of the executives and one that doesn't.

Go to **Log & Report > Traffic Log > Forward Traffic Log**. Right-click on one of the column headings and make sure that the **Policy ID** column is selected, then select **Apply**.



#	Policy ID	Date/Time	Source	Sent / Received
1	3	07:46:28	192.168.13.10	1.11 KB / 10.99 KB
2	3	07:46:28	192.168.13.10	1.10 KB / 9.13 KB
3	3	07:46:28	192.168.13.10	1.07 KB / 9.51 KB
4	3	07:46:28	192.168.13.10	1.16 KB / 12.48 KB
5	3	07:46:28	192.168.13.10	1.12 KB / 11.14 KB
6	2	07:45:48	192.168.13.144	8.41 KB / 10.79 KB
7	2	07:45:24	192.168.13.144	653 B / 4.99 KB
8	2	07:44:57	192.168.13.144	48 B / 0 B
9	2	07:44:47	192.168.13.144	2.51 KB / 1.28 KB
10	2	07:44:47	192.168.13.144	3.49 KB / 5.99 KB

Policy IDs are assigned by the order in which policies were created and so in the example the staff policy's ID is 2, while the executive policy's ID is 3.

In the log, you can see that traffic from the computer with the executive IP is flowing through policy 3, while traffic from the other computer uses policy 2.

Since policy 3 does not have any security profiles enabled, traffic from the executives is not being scanned for security events.